Going Paperless with Electronic Data Safes: Information Ecology Fit and Challenges

Pfister, Joachim ; Schwabe, Gerhard

Abstract: In private households, once received paper-based documents are increasingly substituted by electronic documents. In order to "get organized", an individual nowadays needs to oversee a plethora of digital and physical information items stored at various locations. As a technological solution, cloud-based storage services such as an Electronic Data Safe (EDS) emerge as a home for all digital valuables. In this paper, we analyze how such an EDS fits into an individual's information ecology by drawing upon the results of a qualitative interview study with 39 users of three different EDS services. We develop a typology of the content that is kept safe in an EDS, reflect upon the motivations and upon an EDS's role with respect to other cloud-based storage services individuals are using. The challenges of maintaining a digital, personal archive are depicted and "data value zones" are introduced as a sensitizing concept to reflect upon problematic areas.

Going Paperless with Electronic Data Safes: Information Ecology Fit and Challenges

Completed Research Paper

Joachim Pfister
University of Zurich
Department of Informatics
Binzmuehlestrasse 14,
8050 Zurich, Switzerland
pfister@ifi.uzh.ch

Gerhard Schwabe
University of Zurich
Department of Informatics
Binzmuehlestrasse 14,
8050 Zurich, Switzerland
schwabe@ifi.uzh.ch

Abstract

In private households, once received paper-based documents are increasingly substituted by electronic documents. In order to "get organized", an individual nowadays needs to oversee a plethora of digital and physical information items stored at various locations. As a technological solution, cloud-based storage services such as an Electronic Data Safe (EDS) emerge as a home for all digital valuables. In this paper, we analyze how such an EDS fits into an individual's information ecology by drawing upon the results of a qualitative interview study with 39 users of three different EDS services. We develop a typology of the content that is kept safe in an EDS, reflect upon the motivations and upon an EDS's role with respect to other cloud-based storage services individuals are using. The challenges of maintaining a digital, personal archive are depicted and "data value zones" are introduced as a sensitizing concept to reflect upon problematic areas.

Keywords: electronic data safes, information ecology, data value zones, personal information management, information fragmentation

Motivation and Research Goal

Information fragmentation (Karger 2007) is an ongoing challenge in Personal Information Management (PIM) (Jones and Teevan 2007): The personal space of information (PSI), that spans various collections of information items, is nowadays distributed over devices, as well as physical and virtual storage locations, such as cloud storage or software-as-a-service offerings (Jones 2015). Besides, information items in their physical form are still an important part of an individual's PSI. It is up to each of us to "get organized" and develop strategies for keeping, finding, maintaining, and organizing information items in the digital and the physical world (Jones and Teevan 2007). New services are offered to help safeguard important electronic (or physically born but now digitized) information items, such as multi-purpose, cloud-based file storage services or "Electronic Data Safes" (EDS) (Pfister and Schwabe 2013). These EDS are promoted as the quasi-natural habitat for all "information item valuables" serving as the digital equivalent of a secure filing and organization system for formerly paper-based documents. Moreover, an EDS offers functionalities to receive electronic documents from authorized senders thus serving as another mailbox. An EDS offers features adding supplementary levels of security compared to "ordinary" cloud storage offerings: For example, two-factor authentication and a server-side encryption with a user-specific key are implemented, so that the provider cannot access the data in his data centers (cf. Borgmann et al. 2012).

Electronic document delivery is continually substituting physical letters and there is an obvious trend for going paperless in B2B, G2B and also in the B2C or G2C context: In the postal sector, e-substitution leads to a falling volume of letter mail by almost a quarter since 2004; in 2014 the total mail volume declined by

3.9% on average (International Post Corporation 2015). Therefore, postal service providers as intermediaries are facing tremendous challenges by the ongoing digitization. Besides a reduction in transaction costs for the senders, the recipients of electronic communications (may) benefit from lowered costs for services, a more-timely information provisioning or realizing the dream of a paperless (home) office – something which has been described as a myth in the professional office (Sellen and Harper 2002). Nowadays, information items are directed towards individuals via several different channels which, in turn, contribute to a further fragmentation of an individual's PSI. It is still unclear and has been a blind spot in research so far what PIM strategies are developed by individuals as recipients of such digital documents to cope with this externally enforced trend towards digitization – and how compatible this trend is with already existing personal practices and motivations to curate information items digitally in one's PSI. We want to understand how an EDS is currently used in the field by end users and how it fits in their existing PSI leading to our research question: *Which role does an EDS have in an individual's information ecology?*

In order to answer our research question, we follow an interpretive approach by first trying to understand which content and why users selected this content to be stored in a "safe place". Then, we ask how the EDS fits into the bigger picture of an individual's information ecology. Therefore, we interviewed 39 users of EDS services using a semi-structured interview guide. This resulted in 53 hours of audio data that was transcribed and analyzed using a thematic analysis approach. We invited the participants to give a guided tour in their otherwise inaccessible EDS by letting them voluntarily describe the information items stored therein when they had their EDS opened in front of them during the interviews. Moreover, the participants provided rich descriptions of their information ecology, for instance, which devices and services they use to keep their information items flowing and safe.

Our research is related to "practice theory". Originating in sociology, the turn towards analyzing "practices" (Schatzki et al. 2001) was continuously embraced in other disciplines, such as IS (Cecez-Kecmanovic et al. 2014; Kuutti 2013; Tavakoli and Schlagwein 2016). There is no single "practice theory" but they are considered as a family of approaches sharing historical and conceptual elements (Kuutti 2013; Tavakoli and Schlagwein 2016). Instead of separating the object and subject, practice theory focusses on the entangled relationship between these two entities that are performed in practices which are "[…] routines consisting of a number of interconnected and inseparable elements: physical and mental activities of human bodies, material environment, artifacts and their use, context that contain understanding, human capabilities, affinities and motivation. Practices are wholes whose existence is dependent of the temporal interconnection of all these, and that cannot be reduced to or explained with any one single element." (Kuutti 2013) Following this school of thought, current PIM activities are then practices that are performed by agents using the human body's or the artifact's materiality. In order understand these practices, it is insufficient to focus on micro-interactions, for example, only related to one specific service; the context in which these practices are performed needs also to be taken into account. To achieve this, we based our research on the widely used concept of an *information ecology* (Davenport and Prusak 1997; Fidel 2012; Nardi and O'Day 2000) to analyze and describe human practices (but without relating it to practice theory). In Human-Computer Interaction (HCI), the perspective of an ecology was used to inform the analysis and design of interactive artifacts that transcend individual use by taking into account the complex digital and non-digital context made up by other users and various technological resources (Blevis et al. 2015; Bødker and Klokmose 2012; Jung et al. 2008). As information technology permeates in the private domain and each individual forms part of various socio-technical entanglements, an information ecology perspective allows us to research the relationships between the people who are using technology, the technology itself and how practices are shaped.

An information ecology is conceptualized as "a system of people, practices, values and technologies in a particular environment" (Nardi and O'Day 2000, p. 50). Within such an information ecology, continuous evolution takes place by the multiple levels of influence, for example, if one aspect of the system changes, its effects can be experienced throughout the whole system (Yvette Blount 2011). Such an ecology perspective has not yet been applied to an individual's PIM activities as the "particular domain" which is characterized by information fragmentation. We argue that it is necessary to understand the whole ecosystem of an individual, not only the interaction with single artifacts or services, to identify future design possibilities for PIM activities and services. In doing so, we will gain an understanding of how EDS services fit into the existing landscape of human practices and tools for managing one's PSI. These insights will help designers to develop solutions that reduce frictions in an individual's information ecology, especially when both, the service providers and the individuals, are aiming for going paperless.

The intended audience of this paper are, besides researchers in the domain of PIM, service providers of cloud storage solutions in general, EDS service providers, and organizations in the B2C or G2C context that send information items directly via their portals or services to individuals. Generally speaking, our research addresses every contributor of information items who cares about delivering its services in a user-centered way to alleviate the problem of information fragmentation.

The research contributions of this paper are twofold: First, our findings describe PIM practices with respect to "practice theory". Thereby, we expand the body of literature in PIM on digital possessions through a deeper understanding of users' notions what valuable digital possession are, why they were created or saved from other sources and where they are stored. Second, we introduce the concept of "data value zones". We suggest this as a sensitizing concept for future research involving cloud storage services that provide individualized storage and the ability to share information items. This concept helped us to reflect productively upon challenges we observed empirically in our data.

The remainder of the paper is structured as follows: After presenting related work from the PIM domain and expanding on the concept of an EDS, we present our research context and the approach for data collection and data analysis. Then, findings are described: We start with an insider's view on the types of content before reporting on the user's motivations and portraying their information ecology. Then, the challenges of individuals aiming for a paperless personal archive are presented. In the discussion section, we reflect upon an EDS place in the information ecology. Thereby, we introduce our concept of "data value zones" and discuss some challenges in the field to illustrate its practical relevance as a sensitizing concept.

Related Work

Personal Information Management

How persons keep, organize, and use information items has been studied in the domain of Personal Information Management (PIM) (Jones 2012, 2013, 2015, 2008; Jones and Teevan 2007). As a research field, it is very interdisciplinary because PIM activities are not bound to a specific tool or device but have to be put into a broader context of a "[...] person's integrative use of information across tools and over time." (W. Jones & Ross, 2007, p. 472). It differs from information behavior research because models on information behavior, for example, Wilson's (2000) second model, focus more on how to encounter new information: "However, all these models talk only about how public information is found and ignore what happens after finding has occurred." (Whittaker 2011, p. 4)

Existing research on information organization behavior tends to focusses on PIM activities in specific contexts such as work (Malone 1983) or the professional home office (Thomson 2013), populations such as academics (Kaye et al. 2006) or engineers (Hicks et al. 2008), across devices (Boardman and Sasse 2004; Dearman and Pierce 2008) or about the use of (personal) cloud-based storage (Capra et al. 2014; Marshall and Tang 2012; Odom et al. 2012; Tang et al. 2013). As an exception, the recently published study by Vertesi et al. (2016) takes a very general approach to answer the question "How do people manage their personal data?" which was motivated by the claim of Barkhuus (2012) that findings are often bound to the context of a study and that taking a broader perspective would generate new insights. Therefore, these authors took a general view on the PIM practices and the ecosystems that people engage in to manage their information items. They placed their findings in the wider context of a "moral economy". In doing so, they report on a set of practices, the cultural expectations, affects and responsibilities that arise when people are confronted with a heterogeneous information ecology landscape. In the discussion, we will relate their findings to ours.

PIM activities are not only dedicated to manage hot (immediate) or warm (working) information items (cf. Sellen and Harper 2002) but they, of course, include information items not longer in use. Whittaker (2011) suggested different information properties that influence how information items will be curated: (a) action-oriented items require the user to do something, (b) informative items do not require a user to act, and (c) the uniqueness of an information item is another characteristic. Nevertheless, it is very hard to assess the value of an information item's future worth (Marshall 2007), especially if they do have certain values which change over the "life-cycle" of the item itself and with respect to their owner (Marshall 2011). Since storage costs are inexpensive, the default is to keep all these digital items: "In our analog past, the default was to discard rather than preserve; today the default is to retain." (Mayer-Schönberger 2007, p. 4)

Generally, personal information items are stored with the attitude of "benign neglect" ignoring the consequences or needs of "data stewardship" through deferral to somewhere in the future (Marshall 2007). The strand of research on personal archiving (Hawkins and Kahle 2013; Lee 2011; Marshall 2008a, 2008b) sheds light on these often implicitly occurring practices of forming a digital archive. Moreover, PIM-related research investigates the role of digital possession (Cushing 2012; Kaye et al. 2006; Odom et al. 2012; Watkins et al. 2015) to understand what motivations exist to curate or create collections of information items. So far, to the best of our knowledge, no dedicated research has been performed in order to analyze how people manage "official" information items that had been directed to them, for example, through the use of e-government, e-business services, or just originating by the fact that you are alive and "officially" registered and bound by documents to this world (as the German saying goes: "From the cradle to the grave: forms everywhere."). With our research, we expand the literature on PIM regarding the question if such official documents are forming a distinct part of an individual's PSI and how they are organized, especially, if dedicated storage services like electronic data safes, as introduced in the next section, exist.

Electronic Data Safes

In the domain of e-government, electronic data safes have been proposed to serve as cloud-based services for securely storing documents (Breitenstrom et al. 2008; Klieme et al. 2011; Pfister and Schwabe 2013; Schulz et al. 2010). Besides this secured storage, these services might also serve as digital mailboxes in order to receive documents and share them within e-government and e-business processes. Taking an abstract view, an EDS offers three functionalities: document storage, mailbox-like capabilities of document sending and reception, and the ability to use its content within structured transactions. All this happens under the user-managed access paradigm, that means, that only the safe owners decide with whom and with which service providers they share what information items. Data safes permitting transactions have been called "Active Electronic Data Safes" (AEDS) (Pfister and Schwabe 2015) or Life Management Platforms (Hoffmann and Jäppinen 2013; Kuppinger and Kearns 2013) and are more than "plain" cloud-storage services.

Personal cloud storage services such as Dropbox or GoogleDrive enjoy widespread usage whereas services putting a higher emphasis on security with server-side or client-side encryption, such as Wuala (stopped its operation in November 2015), SpiderOak, or TresorIt (all using the concept of zero-knowledge) seem to be more known and used by security risk-averse users. We posit that an EDS is also a personal cloud storage service because of its ability to upload diverse file formats and being accessible through many devices. It has the potential of being used for sharing documents and files stored therein, but sharing is not mandated. It is offered as one functionality of a cloud-based storage amongst other functionalities such as ubiquitous access, synchronization over devices, and collaboration (Marshall and Tang 2012; Voida et al. 2013). We are not aware of prior research investigating the content of an EDS or a trustworthy cloud storage provider.

The mailbox and transactional aspects of an EDS can be related to the domain of electronic bill presentment and payment (EBPP) and electronic document delivery by postal services. As noted by Hildebrand (2015), a possible transition path is evident: from (1) manual invoices sent by postal letters, (2) to semi-automated processes using PDF documents as invoices sent by e-mail or through provider specific portals, and (3) to, finally, a fully, end-to-end integrated order-to-payment process. For the senders, electronic documents have huge advantages by reducing transaction costs. However, on the recipient's side, it has not yet been investigated whether "going digital" reduces transaction costs in form of a less burdensome PIM. Our study helps to understand what role does an EDS play when end-users have to organize electronic documents – and still are bound to manage existing or still newly arriving physical documents at the same time.

Research Method and Empirical Context

Empirical Context

Semi-structured interviews were used to collect data from 39 users of three EDS services. These three EDS service providers were contacted by the authors of this paper and asked if they supported this interview study by helping to recruit participants. Two of these service providers are Swiss based and are run by private companies (service A and B). The third EDS provider (service C) is part of the Austrian E-Government infrastructure and is run by a private sector company. The authors of this paper worked independently from the participating EDS service providers; no conflict of interest or financial dependencies existed.

EDS service A is marketed as a safe location for storing documents and passwords to access them everywhere. The service is offered for free and native apps for iOS and Android are provided but no client for automatically synchronizing documents. *EDS service B* presents itself as a general purpose, secure online storage provider following a freemium pricing model. A password safe is offered and, as well as for the files, it is accessible via native iOS and Android apps. This service offers a client for synchronizing files automatically over various platforms. *EDS service C* is provided as a data safe within the context of the Austrian e-government infrastructure. It is bundled with an e-identity component of a digital signature and has got a freemium pricing model offering a safe space for storing and digitally signing documents.

The participants were recruited by self-selection and answering open calls for participation in an interview study advertised for about ten days either on the EDS's login page (service B) or announced in the news section after logging in (service A). The participants were offered a small gift. This resulted in the recruitment of 20 (EDS service A) and 16 (EDS service B) participants. For EDS service C, recruitment took place using an open call for participation on Facebook offering a small gift which three participants welcomed. The interviews were carried out via Skype, Google Hangout or telephone except for two interviews that took place in the participants' homes due to geographical proximity where the researchers were located.

Data Collection

The interview guide for performing the semi-structured interviews has been pre-tested to optimize the wording and flow of the questions and to ensure a reasonable length-depth ratio of the interviews. The interviews were audio-recorded. After asking some demographic data, the participants were invited to *draw their information ecology*, an approach that was inspired by Kaye et al. (2014). By asking "Where do you store digital information in the cloud?" and letting the participants draw their information ecology, they were better able to reflect upon the services they used. Then, the participants were asked to *give a guided tour* of their electronic data safe and its content, an established and widely used method of inquiry in the domain of PIM (Jones 2015). Therefore, the interviewees had opened their data safe during the interview. They were given full control over their privacy and confidentiality by only telling the interviewer about the content elements that they felt safe of. The interviews continued by asking about practices surrounding the reception and the processing of electronic documents, and how paper is handled.

In total, 39 interviews have been conducted (31 in German, 8 in English) resulting in 53 hours and 02 minutes of audio data. One of the authors transcribed all the interviews. On average, an interview's duration is 1 hour 19 minutes and it contains a net number of 4079 words without the questions asked. The participants came, due to their self-selection, from various backgrounds and had in common that they actually used a specific EDS. 34 males and five females took part and the average age is 41 years (25-29: 4; 30-34: 6; 35-39: 3; 40-44: 7; 45-49: 7; 50-54: 6; 55-59: 3; 60-64: 3). Everyone used at least one smartphone.

Data Analysis and Interpretation

After the transcription of the interviews, thematic analysis (Braun and Clarke 2006) as a method for analyzing the interview data was used to answer our research question: *Which role does an EDS have in an individual's information ecology?* This method has been successfully employed as an interpretive research paradigm in HCI (Vincent et al. 2014) to uncover themes systematically. The method is closely related to grounded theory (Glaser and Strauss 2009; Strauss and Corbin 1998) and it can be used in a realist (essentialist) or interpretive (constructionist) way. Its principles are equivalent to a hermeneutic approach. The research in this study is conducted within a constructionist framework. We proceeded inductively in a data-driven fashion without an apriori attempt to fit the data into theory. Thus, observations are interpreted to uncover latent themes – to use the terminology of Braun and Clarke (2006). They represent hypotheses about underlying motives why certain information items are stored in an EDS. Furthermore, they indicate how an EDS fits into an individual's information ecology. We conceive that the positioning of services in an information ecology is related to existing and newly developed or adapted practices.

To maintain rigor, we followed the six phases as described by Braun and Clarke (2006): The interviews, as well as the transcription, were conducted by the first author of this paper which allowed him to immerse deeply in the data by performing these steps himself and re-reading the data several times (phase 1: familiarize with the data). The analysis was assisted by using the software MAXQDA. Initial codes were assigned using open coding (phase 2). Axial coding was used to identify themes by collecting codes into potential

themes (phase 3). Internal validity was assured by iterating between identified concepts, the assigned codes, and themes several times, paying attention to reflect upon the researchers own perceptions and preconditions that might influence the research process (phase 4: reviewing themes). We did not opt for coding the data set independently by another researcher based on the understanding of coding as an active and reflexive process and that no exclusive reality in the data can be captured by assigning codes which would be more a realist assumption. An internal research report was written by the first author which served as a means to define and name themes (phase 5 and phase 6). Then, discussion with research peers and the other author proceeded to validate and refine the discovered themes before this article was compiled.

The aforementioned six phases do also cover the criteria for qualitative research conducted in information systems research developed by Klein and Myers (1999): (1.) "The fundamental principle of the hermeneutic circle" is achieved by iterating between data, composing intermediate reports and discussing the results with peers. This is covered by phases 4, 5, 6 of Braun and Clarke. (2.) "The principle of contextualization": By relating our findings to prior research in the domain of PIM and asking our participants questions about other services besides going in-depth into their EDS usage, we were able to contextualize our findings. This is covered by phase 5 and 6 of Braun and Clarke. (3.) "The principle of interaction between the researchers and the subjects": In preparing the interview guide and pre-testing it, we gained initial experience in how the interview study participants would react. During the interviews and the analysis, we paid attention that the observations guided the sense-making process and not own assumptions. This is related to Braun and Clarke's phases 1, 2, 3, and 4. (4.) "The principle of abstraction and generalization": During the analysis, we related our findings to existing theories of PIM and discussed them in the light of an "information ecology". This refers to refining the findings in phase 6 referenced by Braun and Clarke. (5.) "The principle of dialogical reasoning": Our analysis was not guided by preconceptions. We paid attention to let the themes develop from the data and anchor them therein. This took place by discussing emerging themes with peers and compiling intermediate reports. This is related to phases 4, 5 and 6. (6.) "The principle of multiple interpretations": If contradictory interpretations emerged, we tried to resolve this by going back to the data and check the context before discussing and agreeing upon an interpretation. This was performed in Braun and Clarke's phases 3, 4, 5 and 6. (7.) "The principle of suspicion": In order to avoid possible distortions arising from the narratives of the participants, we tried to design the semi-structured interview guide to focus on the area of interest as the main part (EDS) but as well as the context (information ecology) and clarify ambiguities during the interviews immediately. By combining the "local" EDS-view with the "global" contextual view, we reflected upon potential biases in the phases of analyzing and discussing the findings. This was performed in the phases 4, 5 and 6 proposed by Braun and Clarke.

Concerning the ecological validity of our findings, we follow the distinction made between representativeness and generalizability as the two components of the ecological validity (Kvavilashvili and Ellis 2004). Representativeness refers to the "naturalness" of a situation. We achieved this by asking the participants to have their EDS opened during their interview. Generalizability is obtained by taking into account the information ecology as described by the participants, and by contrasting this landscape with findings from our in-depth study focusing on the content of an EDS. During the interviews, we asked for clarifications when any ambiguous statements had been uttered, and we asked deepening questions so that the participants could elaborate upon their usage preferences and the distinctions they made concerning their choice of service. This understanding, taken together with our data-driven approach, gives us the confidence to have achieved generalizable findings. Especially, we did not have any pre-conceived assumptions that sharing in an EDS will or even must take place which is commonly associated with any cloud-based storage services. Therefore, we argue that the findings have been elaborated without theoretical distortion. The quotes in the following sections have been translated by the first author when they originally had been uttered in German.

Findings

Our findings have been developed in a bottom-up and data-driven fashion. We first report on the type of content that is stored in an EDS before we report on the motivations why these information items were stored therein. Then, we present the context marked by other services that are used to store information items. Finally, we report on the curatorial challenges of going paperless.

Typology of Content Stored in an Electronic Data Safe

Comparing the three EDS services and the content people reported to store in an EDS, no big difference seems to exist with respect to the types of documents. We clustered the content types according to overarching topics based on their frequency and the importance attached to them as expressed by the interview participants. Two main categories of documents can be identified: "common" as the primary category and "selectively stored" as a secondary category. The reasons, why documents were kept, will be reported upon in the following chapter. The category of "common documents" is characterized by documents relating to an individual's financial status, official and physical existence, possessions, needs for protection, and being bound to legal duties. These categories have been utilized by nearly all participants. The second category of "selectively stored documents" refers to additionally stored items due to personal preferences.

Common documents: Within the primary category of "common documents", we noted that nearly all the interviewees did scan their passports, ID cards or other documents that have been issued by official bodies to certify and document an individual's existence. These scanned ID documents were regarded as being very valuable and helpful, despite a scan lacking the legal qualities of the physical original. Official documents that were issued by authorities to prove a certain legal status, right or communicating a formal decision for an individual as a citizen were stored within most of the EDS of the participants. These documents relate to an individual as an official proof that it has been taken care of and that it has been registered with official administrative or governmental procedures. In the same cluster dealing with these "common" documents, everything related to living somewhere, either rented or in owned property, will be subsumed therein. This encompasses regular statements of utility companies as well as documents that justify the right to stay somewhere (rental contracts) or plans of the real estate.

Documents related to the financial life of a person were stored in an EDS by nearly every participant. Especially monthly statements and general banking documents were kept safe there, thus proving that someone has financial powers. In this cluster, documents related to retirement pension plans are stored. Documenting possession by digitizing receipts, invoices or warranty documents was performed by the largest part of our participants, too. The merits of existing and being financially potent to buy things of value entail a need to secure these possessions by documenting ownership. Furthermore, if something should happen, the documents in this cluster might help to exert warranty claims or to deal with insurance companies. Protecting oneself against the loss of possessions and against various risks entails safeguarding this kind of "protection credentials" which are forming part of this cluster. This also pertains to documents issued by insurance companies, such as contracts. Nearly half of the participants stored such documents in their EDS to have proof of the fact and the details on how their life is protected. Another cluster of documents is formed by legal documents binding someone to obligations imposed by law (taxes) or self-inflicted obligations due to entering contractual, thus legally binding, relationships, be it business-wise or on an interpersonal level (for example, a marriage contract).

Selectively stored documents: In this category, several participants remarked that they are managing *other people's data* within their EDS. In most cases, one partner acted as the digital custodian of the partner's or family member's data, for instance, scans of ID cards. One interviewee mentioned that he stored all the documents related to his function as a legal guardian for several people in his EDS. *Health-related* documents, such as insurance policies or general documents issued by a health insurance company, were commonly referred to as belonging into an EDS; but they have not been mentioned so regularly compared to other kinds of protective contracts. Health records have only been stored by one person in an EDS whereas some more tried to keep their vaccination record up to date in an EDS. All documents on *traveling* enjoyed a wide acceptance and storage in an EDS. The main motive behind having such documents in an EDS was to be able to retrieve them in the case of need, maybe due to theft. Reservations and booking references, as well as copies of passports, etc., were commonly reported to be prepared in advance. *Other leisure-time activities* with a need for entrance tickets or general activities in associations or clubs also produced some documents that the participants wanted to keep safe in an EDS. Keeping and organizing *invoices* involves another category of documents. The breadth and depth of collecting invoices are highly individual. Participants noted that their personal schemes for organizing digital items are either thematically or pertinence-based. Still, a folder containing *miscellaneous items* often existed. Some of our participants are self-employed. For those, storing business-related data, maybe even containing *customer data and project data* as well as invoices or offers, an EDS was judged to be a suitable location for keeping such sensitive information items "in the cloud".

Although an EDS offers the potential to store every type of information, it was rarely used to store memorabilia, that means, items to evocate past events in future encounters. Only very few participants elaborated on "really private data", for instance, photos or videos, that they stored in an EDS. Other categories that have been identified in the category of "selectively stored documents" are about *job applications* for which the current and previous versions of a CV have to be accessed and stored, *mobility-related* documents such as car leasing contracts or invoices from a garage. *Job-related data* was also kept in an EDS such as work contracts, schedules or locations of specific service points of a company that a mobile worker needed to access. Only a few participants explicitly named to have an *archive folder* where older data items, for example, from a former company the participant owned or a PhD-project, were stored for eternity. Another participant reported storing all document related to renting a property under the legal construct of a non-trading partnership with his siblings in his EDS which has to him an archival meaning. Other participants reported on storing information items about services they had subscribed to in an EDS.

Passwords: Besides storing documents or files, the dedicated password management functionality of the EDS services was used, too. Therein, surprisingly, not only passwords were stored. Our participants used it also to help to memorize PIN codes for mobile phones, tax identification numbers, membership numbers, notes, personal goals (as mantras), software license keys, factual information such as fashion sizes or the size of a mountain bike wheel. Some participants stored this not in the password safe but as regular documents. When participants estimated the number of passwords, their answers ranged from a few to more than 150 passwords (one participant used an encrypted spreadsheet file with more than 400 passwords).

Motivations for Storing Digitized Content in an EDS

In the interviews, the participants were asked to describe the character of the information items they store in their EDS. Furthermore, we asked why they digitized physical documents – regardless of where these information items have been stored afterward (see Table 1). The main motives are listed first.

motivations for storing content in an EDS	motivations for digitizing documents
safeguarding sensitive data	protection from loss
digital filing system/aspiring to the paperless office	aspiring to the paperless office
protection from loss	ubiquitous access
preserve long-term static data	greater accessibility
ubiquitous access	using in digital transactions
store everything and dynamic information items	saving physical space
reducing cognitive burden → passwords	digital copies help if a physical original is lost
	improves sharing capabilities

Table 1: Motivations for storing content in an EDS and for digitizing documents

In general, an EDS is considered as a *safeguarded digital home for sensitive data*. The participants expressed a huge variety what constitutes "sensitive" documents to them. For instance, financial statements were classified by some participants as very sensitive whereas other participants took a stance that such information is not so important. An EDS is also seen as a tool that helps in the transition from a physical to a digital filing system for general paper works, helping to *strive for the ultimate aim of having the paperless (home) office*. Some interview participants reported that their only location for storing scanned and newly arriving documents is the EDS. Such a tendency to unify everything in one place (as the physical filing system had served this purpose before) highlights the desire to avoid information fragmentation ("[Scans of documents] are stored only in EDS service A. They still exist as paper. What would you recommend? If you do that [auth.: store them locally] then you will have stored things in parallel in 7000 locations again. But I think that the EDS service A should be sufficient.", A17). EDS services offer secure storage to *protect the stored information items from loss*, especially for *long-term, static data* ("That are mainly documents that I consider to be important and that I do not like to disappear because of a fire or a flooding. If my house burned down, I need those documents.", B02 or "Documents stored in EDS service A have the potential to be needed sometime again in the future in order to look something up or for the taxes.", A02). This category was informed by the distinction the interviewees made between "dynamic" and ephemeral data and the preservation of "long-lasting, stable" information items such as digital copies of passports. Moreover, having ubiquitous access to one's data (every device, every place) was given as a motivation by only a few participants (5/39). And two participants thought of an EDS as a home for really everything digital they own;

this also encompassed dynamically changing items, notably any files and documents that they create ("I thought, I will not make a difference anymore between storing documents in a safe and storing documents securely – in consequence, I will use [my EDS service B] for everything I am working actively with.", B16).

Each of the analyzed three EDS solutions gives the users the capability to store their passwords in the EDS which was actively used by 26 participants. Only service B offers an app that can be accessed offline to access the passwords. The main motivation for adding passwords to an EDS was to reduce the cognitive burden caused by the efforts to remember (ideally) individualized access credentials for each service. A centralized and seamlessly integrated access to their passwords has been reported by the interview participants to have positively improved their password management habits resulting in increased security.

Central motives of an EDS's usage are reflected by the motivations to digitize physical documents, too. The motives of "protecting from loss" and "aspiring to the paperless office" have been uttered equally prominently by the interview study participants. The motivations to digitize documents focus more on the beneficial affordances of digital information items such as their potential re-use in digital transactions. Albeit the motivation of having *ubiquitous access* is less prominently reported by EDS users, they still see this as a huge motivation to digitize documents ("So, here is an example, you have got a confidential document like a driver's license that I now have got as a digital image in the cloud. Just in case I forget it, I could tell the police and show my driver's license as a picture.", B14). The dematerialization of information items as digital replica offers new affordances that overcome burdens associated with paper: digital information items are *more accessible*, for instance, by using full text search mechanisms ("I am massively faster compared to the time I had to look in folders through paper. Using the search function, I'm really faster now.", A12); they can be *used in digital transactions* ("I will add the [scanned] documents to certain business processes.", C02); they help *saving physical space* ("I had to reduce the space for document storage and folders by a third due to moving. When possible, I scanned and destroyed everything. I did this radically.", B08); they are *helpful in re-issuing physical documents* if they got lost ("Obviously, the [legal] value is not there. But if you have to redo your passport and lost it, or your passport gets stolen, usually they will ask you for a number.", B02); and they *improve the ability to share information items* easily.

When we asked the participants what should not be stored in an EDS, half of the participants agreed that (almost) everything could be stored within such a service – if they trusted it. One participant – albeit using an EDS – mentioned that nothing should be kept in such a service because data would be given out of one's hands. In between these two extremes, the participants discerned two groups of information items that should not be stored in an EDS: high-impact and low-value data. As *high-impact data*, the participants thought of (a) financial data like balance statements, credit card data or – given as an example – documents confirming that they had been tax evaders, (b) information items that could be used to start transactions ("I would not save something in an EDS which could give access to other data. In case of doubt, I would not store the CIV code on the backside of my credit card." B10), (c) information items that could be used against oneself, and (d) various high-impact information items such as diaries, business-wise classified documents, contracts with attorneys, or documents related to the immigration in another country. As *low-value data*, the participants thought of saved journal articles, manuals, mundane invoices or own prose ("That would be everyday things. […] A bill from the dentist, if it's not relevant for taxes, I surely will not upload it into EDS service A.", A11). Interestingly, multimedia information items (photos and videos) were explicitly exempted from belonging into an EDS by a few participants. The main reason given as an explanation was the lack of reasonably priced storage space provided by an EDS that would be needed for huge amounts of photos ("Pictures do not go in there because that would blow up the data volume.", B01).

A Still Life of an Information Ecology in the Presence of an Electronic Data Safe

EDS are used by the interview participants predominately for private purposes. Three out of the 39 participants used their EDS mainly for professional purposes, and all four self-employed participants mixed their private and professional information items in their EDS. To get a better understanding how this usage fits into the greater picture of other services used, we report on the "information ecology" of our participants in which other services are used, too. In doing so, we deliver a kind of differential diagnosis of the information ecology: the EDS vs. other services. The previous section depicted why an EDS is used through analyzing its content and the motivations of the users. In the discussion section, we will take all the information together to reflect upon the positioning of an EDS in the information ecology.

Google's services are used for private reasons by 21 of the 39 participants, whereas GoogleDrive was used by twelve interviewees. They reported that they used GoogleDrive mainly for saving and having a backup of photos, for instance, by using the automatic synchronization feature of their smartphones. The participants did judge GoogleDrive as a storage space for "unimportant" data that will be public afterward anyway or because they have no transactional value ("But this is all stuff that does not exert a higher level of privacy.", B12). Sharing and collaborating was also the main emphasis how the participants described their main usage of GoogleDrive. Especially in the context of leisure time clubs (they were sharing out of print music scores), for students during their studies, or parents collaborating for school-related activities, GoogleDrive was preferred. Six participants explicitly stated not wanting to use GoogleDrive. GoogleDrive and GoogleDocs (formerly marketed as a separate product but now integrated into GoogleDrive) were seen as ideally complementing services because documents can be edited very easily, transgressing borders of devices, thereby eliminating the need for re-uploading an edited document.

Dropbox as a dedicated cloud storage service was used by individuals in a private context mainly for sharing photos (17 of the 39 participants) either with friends, family members, or for transferring documents. Automatic synchronization is used by five participants in order to keep several devices in sync or to have a backup in the cloud. In a professional context, Dropbox is used by five of the 39 interviewees. The main motivation reported by all interviewees was that Dropbox works seamlessly: it is available across devices and operating systems and offers a ubiquitous access to one's data. Moreover, this service is favored because it is the first one of its kind and, therefore, well known; due to its seamlessness, is judged as being easy, comfortable, and – very importantly – being free or modestly priced.

The participants also reflected on potential inhibitors of Dropbox's usage. The syncing client that has been viewed as a positive asset was judged by other users as an unwanted and aggressive way of uncontrollable data extraction out of their personal space of information into some far away location in the cloud. Other disadvantages were seen in the size limitation of the service or that job policies are forbidding its usage. The most compelling reasons for avoiding Dropbox was expressed by the participant's perception of their data stored in Dropbox having the character of being only a guest on a public space. The lack of encryption, the server location, and the company being domiciled in the U.S.A. evoked feelings of insecurity which especially became apparent for the interview participants alongside the revelations surrounding the publication of NSA-activities by Edward Snowden.

Nevertheless, the participants in the interview study frequently referred to as Dropbox being the gold standard when it comes to ease of use and seamlessness. To overcome security concerns, people shifted selected information items to other services (such as EDS service A and B), or only "unimportant" information items were stored there, like invitations, leisure-time related activities, cooking recipes or brochures. Still, backing up and synchronizing photos were used by 14 of the 39 participants; one participant added that only non-compromising pictures would be stored ("I mainly use Dropbox for private pictures, but not really private ones. If I share pictures via Dropbox or services alike, I do always question myself if I could cope with it when these pictures could be seen be someone else. If I am confident, I'll use Dropbox. Otherwise, I'll use encrypted e-mail or whatever else.", A13). Storing travel-related documents, scans of passports, or ID documents in Dropbox was also performed frequently – which was based on the ease of access if needed. Only one participant used Dropbox as his main storage for everything. Concerning "more private" data or "sensitive" data, six participants of the 39 participants in total stored valuable data in Dropbox which are: synchronizing their encrypted password manager file across devices, medical information of the daughter, a patient living will, invoices, job applications, pension plan documents, documents from others (parents, spouse), and some other "important" documents not described more closely.

Apple's iCloud-based services were used for private reasons by twelve out of the 39 participants. Five participants tried to consciously avoid these services because they felt a lack of control where their data was stored and had less trust in the company Apple or any company that has to follow the U.S. Patriot act. Five participants store documents or synchronize all their documents via the iCloud; eight participants used the iCloud to store their photos. The participants reported upon the reasons for using the iCloud which are mainly based on the ease of use by synchronizing and having a backup at the same time in the cloud. Remarkably, one participant misused iBooks to store all her documents in there.

Microsoft's OneDrive is used by ten of the 39 participants in this study but usage reports are far less extensive, and this service seems not be as widely spread as other cloud storage services. It is mainly used within a professional or self-employed context (four participants); only two participants used it in their

private context but only for "unimportant" documents ("OneDrive is for my documents that are not confidential or secret. If some hacker was there, I wouldn't care. There is no secret.", A20). One participant noted that he will move from OneDrive to EDS service B in the future because EDS service B seems more secure to him. Another frequent user in the business context said, he only puts selected content in OneDrive that is not so critical. The main argument why the participants got into contact with OneDrive is its bundling with Microsoft Office – and a feeling that it cannot be avoided ("I had to use OneDrive because it was kind of prescribed by Microsoft.", A15).

Evernote is another service that is used by five of the 39 participants in the private context and by one other participant in the professional context. The usage patterns encompass note taking (long and short term), backup reasons, tracking things, or Evernote containing the entire document archive (one participant; the information items do match the categories what the other users stored in their EDS, see section "Typology of Content Stored in an Electronic Data Safe"). Notes were the predominant content type, but also documents that needed to be accessed ubiquitously or providing access credentials were stored. One participant recorded his fashion sizes (collar size, jeans size) as notes. Again, having travel-related documents at hand just in case if something was needed was a usage pattern exhibited by three interviewees.

Other service providers: The following services are used only by one participant each. *Hubic* is used to synchronize data between devices and to share photos with family members. For multimedia content, participants also used *Facebook*, *Flickr*, *ImageInvent*, Deutsche Telekom's "*Mediacenter*" or *WeTransfer* to store and share larger amounts of data. *SugarSync* is used as an online backup of pictures by one participant which was favored by him because the syncing client can be configured to sync directories independently. *Wuala*, a cloud storage provider with client-side encryption, has been actively used by three participants during the time of the interviews. Seven other participants had used it temporarily before but abandoned. The main negative issues that were voiced by the interview participants were a complicated user-interface, a difficult handling of mobile up- and downloads, and the fact that the once free service became a paying one. As huge benefits for this service, the client-side encryption and being a Swiss service have been remarked by the interviewees repeatedly.

Running own servers: One interviewee reported that he is using his *own RAID* to store all of his data. Three participants administrated in former times an *own server running cloud services*. They reported having given up on this because regular maintenance became too time-consuming. Additionally, they argued that the benefit of resorting to professionally run services is the freedom from caring for everything yourself. Another participant even dismissed the general thought of self-administrating servers as too time-consuming – he just wants a tool that simply works.

Curatorial Challenges of Going Digital

This section reports on the challenges that our interview study participants experienced to maintain and keep their information items flowing in their information ecology.

Digitization of existing paper: A common challenge expressed by the interviewees was the initial effort that is necessary to put existing documents as scans into an EDS. Another challenge experienced by the interviewees was, what they should do with the physical original after scanning. Our participants expressed a tendency to keep "valuable" paper if it has legal value (with a signature or a stamp) considering these as *unique originals* ("I am reluctant with my reference letter from my employer. If it is clear that I will need it electronically, I scan it. I would not destroy the original.", A07). On the contrary, *bulk items* (warranty certificates or receipts) maybe having a scanned signature (insurance policies) will be destroyed after scanning ("No, I did throw away the originals. So what? You can print them again anytime.", A12). Still, some participants expressed insecurity about the best approach in the future, leading them to keep, for instance, paper receipts to deal with warranty issues in the future. Another challenge was described by the participants with respect to retro-digitizing existing valuable documents. Unless they are not needed in electronic transactions, our interview participants judged this pro-active scanning as too laborious. Moreover, the interviewees suggested an "on demand" approach of digitizing when something old is needed ("I would digitize reference letters when I would need those.", A19). Some participants feared that paper-based information items will become inaccessible after their transitioni to a digital filing approach ("Starting September this year, everything new will be scanned; what exists before this date, I will leave it untouched. If I needed to digitize everything in retrospect, I would need to take two to three weeks of vacations.", A19).

Six of the 39 participants had a "digital only" strategy, that means, that they scanned everything which was a physical document: "I've got no paper folders, no envelopes. If it is important enough that I will keep it, it gets scanned." (B05) Or: "I do not like to make exceptions. If I go for electronic storage, then the full way." (B08). Notably, going fully digital seems to coincide with having the right scanning equipment which will serve as a catalyst. All the participants with a "digital only" strategy used a scanner with a document feeder: "Then I bought a new scanner. It has an automatic document feeder. Then, I thought, this is really fast – I can do this extensively. Now, once a month, I will process the paper. This is very fast." (B08) Some of these frequent-scanners expressed that scanning became an automated routine ("I have got such a multifunctional device with a duplex scanner built in. Over time, scanning became a routine.", B11). The scanning avant-garde of our participants expressed their favor for having a paperless office. Nevertheless, they mentioned some challenges arising from this strategy: First, they have to remember to update content if new documents arrive physically ("And it is just a matter of keeping things updated. For instance, if I have got a new life insurance or a new insurance policy. I would have to think not to forget to put it into EDS service B.", B02). Second, if collaborators need to have access and are not using an EDS or prefer paper, something needs to be printed again ("As long as I am working alone, it is easier. Limits exist, for example, when my mother didn't have access anymore. She wants to have the documents that is why I suddenly need paper. I have to print it for my mother. It became more complicated through this.", B08). With relation to the information ecology as a metaphor, this is an ideal example of coevolution: social or technological spheres repeat their evolution cycles in order to adapt to and benefit from changes in the environment.

Document providers are used implicitly as outsourced storage: Document providers or issuers, such as such as credit card or utility companies, are mostly companies in a B2C relationship with the document recipients. They will send documents to individuals by e-mail, the provider's specific portal or within an individual's e-banking portal where also the payment can be executed. Our participants showed four strategies to manage these information items sent to them: (a) let the documents be stored at the service provider (20/39), (b) download documents from a provider and store them using cloud storage services (15/39), (c) download documents from the provider and store them locally (14/39), and (d) download documents from a provider and store them locally and in the cloud (10/39). Preference for downloading was given to account statements or any other financial documents bearing relevance for the tax declaration.

The majority of our interviewees seem to have outsourced parts of their personal archive by taking a laissez-faire approach. The underlying assumption is that the individuals assume that the service provider will be responsible for taking care of these personal documents. In the extreme, a provider's portal is considered to be an eternally accessible archive – something that reflects the outsourced curation of a distinct collection. This finding is underpinned by the judgments our participants expressed towards the question how long documents will be kept by the service provider. This revealed a broad spectrum of impressions: some participants (7/39) expected the service provider to archive the documents for eternity, some others (5/39) guessed that this will be not forever, and some others guessed that the limits might be in a period within half a year to three years (4/39). In contrast to these outsourcers by laissez-faire, we identified a loss-aware subgroup of interview participants that prefer downloading all documents. The main motivation was to have information items under one's own control because the provider might not store them forever or even delete something ("Yes, I want to have these things with me, for example, if the provider should change something. Maybe documents will only be kept two years by the provider. But I would be independent then. If I should need something and could not have access to it, that would be cumbersome.", B11).

We assume that an assessment of impact is made on how severe the loss of the documents or the loss of access to them would be ("For example, when I will contract for financing real estate involving a huge amount of money, it is not sufficient to keep it only at the bank for me to access it probably somewhen. Let's put it this way: I would like to have this proof still with me.", B12). Moreover, this impact-based assessment and the (un)intentional delegation of long-term storage can be interpreted as a coping strategy in face of an increasing information fragmentation: "I have come to the point of using too many cloud services, and it got confusing." (B13) Besides avoiding to download documents oneself, our participants expressed their desire to have all important documents at one centralized location – something that has been achieved before with physical documents and their grouping into folders in a home office.

Providing access to others: We observed an unexpected pattern of a "share everything" approach: Some participants shared their individual access credentials with their partners, including all passwords stored in the EDS. They had the notion of having one family account which is shared by persons all having the

equal rights and reasons for accessing the information items stored in there ("I have got nothing to protect against my family, my son has all my passwords. We are one family.", A20). Instead of relying on technology to control this information sharing, it was replaced by social trust, often justified to prepare for fatal incidents or reasons of convenience to having everything stored in one place. This revelation of access credentials reflects currently enacted sharing patterns prevalent in the family or marital relationships: "Of course, my wife has access using my username and password. We shared it. I have got not security concerns about this. You have to tell someone, of course, just in case something should happen." (A03). Documents related to the last will are also shared, sometimes by deliberately revealing all credentials during an EDS owner's lifetime – trusting that the recipient will not misuse them ("I gave him [my brother] access to my whole data safe and he gave me access to his because you potentially could die. I would have done this also with my tax lawyer but only in a restricted fashion.", A15).

Discussion

In the following sections, we discuss the positioning of an EDS in an individual's information ecology. Based on our findings, we introduce the concept of "data value zones" as a sensitizing concept. We then reflect upon areas of challenge and tensions that seem to be inherent in cloud-based storage solutions that have a strong focus on personal information items that might become potentially shared information items.

The Role of an EDS in an Individual's Information Ecology

In order to answer our research question "*Which role does an EDS have in an individual's information ecology?"* we started by taking a look at the content stored in an EDS. Our typology revealed that an EDS is the primary home to "common" and "selectively stored" documents as well as transaction-permitting passwords. The nature of most of the documents can be described as digitized unique information items, such as certificates or reference letters thus reflecting the information property of uniqueness suggested by Whittaker (2011). These documents were scanned voluntarily for their use in electronic transactions (as action-oriented information items, cf. Whittaker (2011)), or to prevent loss of "digital originals" or digitized content. Our participants expressed that these information items are of higher value to them. Therefore, we argue that the content in an EDS serves as a collection of selected, high-valued information items for which a conscious keeping decision has been taken. Only the participants who used the synchronization client to automatically upload all their documents and store these entirely within EDS service B did avoid the problem of assessing the value of documents. In their continuous usage of the EDS as a synchronization and backup tool, they followed a keep-all approach implicitly deferring the hard to take keeping decisions, something that has been reported to be common for the curation of personal information collections in both, the digital and analog world (Marshall 2008b; Whittaker 2011).

Temporal aspects of managing information items have been covered in the PIM literature mostly as a dimension for the retrieval (Jones and Bruce 2005). However, newer findings suggest that these temporal aspects are less prominent than other characteristics for re-finding documents (Xie et al. 2015). Nevertheless, our data suggests that there might be some overarching dimensions of information properties that describe the information elements stored in an EDS: informativeness, action-orientedness, uniqueness (cf. Whittaker 2011), and new: periodicity and subjectively assessed value. For example, statements of banks arrive on a regular basis and are archived by a user in an EDS due to their uniqueness (personalized information), their informativeness (current balance), and possible action-orientedness (for example, if fraudulent transactions are reported), therefore bearing a subjectively high value. These dimensions are overlapping, and their assessment might change over time due to external factors. This also makes it hard if not impossible to generalize, for example, a user journey or behavioral model with respect to the content types. For instance, banking statements might become a piece of evidence in the process of getting divorced to identify whom of the partners contributed to which extent to their mutual income and wealth. Such a potential need for an unanticipated use also fosters the tendency to store everything and defer all the difficult keeping decisions. In the light of an unknown future, it is hard for individuals to decide which information items need to be kept based on some vague and dynamic characteristics. This also goes along with the ecology view which emphasizes the interdependent nature of the ecological system with its actors. Furthermore, such a fluid perspective is in line with the notion of a continuum thinking in archival science where records – or in this case information items – are "always in a process of becoming" (McKemmish &

Piggot (1994), cited by McKemmish (2001, p. 334)) and are not strictly following a life-cycle with linear phases. Future research might identify further characteristics explaining these difficult keeping decisions.

It is an interesting observation, from a content perspective, that in the category of "selectively stored documents" the participants in our interview study managed information items for others. This indicates that "personal information management" becomes group information management within an EDS. Sometimes, this is done on purpose and with full consent, for example, the couple who decided that he will manage some parts of the electronic paperwork, and the spouse will take care of the other documents and the accounting. With respect to that insight, we even argue that an EDS can be interpreted as a transactive memory system (Wegner 1987): Each partner has his or her specialization, and they coordinate, for example, to organize and to retrieve documents for taxes, by resorting to a shared memory, the EDS. Both collaborators establish credibility in each other's capabilities of managing information items for a given task.

Protecting from loss was the main motive for using an EDS alongside with motives to get rid of paper documents to avoid a cluttered home. Therefore, an EDS serves as the centralized locus of curated, high-value information items needed in a long-term perspective. It can be characterized as a centralized, trusted repository uniting different digital assets from various origins – but, nevertheless, it is not the only service in an individual's information ecology! This goes along findings in prior research (Marshall 2008b) that people will use several services due to various reasons and affordances despite speaking about their desire to have everything centralized in one place. Now, we can interpret this behavior in terms of an information ecology: a monoculture would provide short-term benefits but would be rather detrimental in the long run. When all access passwords are put into an EDS, it acts as a catalog of all digital belongings that are accumulated and distributed in an individual information ecology (something that has been suggested as an alternative to a centralized storage by Marshall 2008b). Storing multimedia data or sharing information items is organized via other services that seem more appropriate, for example, due to sophisticated functionalities or the fact that they are free of charge. Our participants used mainstream cloud storage services only for "unimportant" data when an EDS is present. The affordances of Dropbox as a seamlessly integrated tool into the operating system made it the predominant choice for sharing photos. When collaboration was needed, GoogleDrive was favored for editing documents. Microsoft's OneDrive was preferred in a business context. Our participants formed islands of collections, and they attributed special use cases or preferences to each distinct storage location. Generally, non-European service providers were often regarded as being less secure than European services which also is also reflected in the choice of services and the distribution of high-impact data in an EDS and low-valued and shareable data stored in non-European services.

Introducing Data Value Zones as a Sensitizing Concept

Our research question aims at identifying the role of an EDS in an individual's information ecology. Since our research approach is interpretive, we are now trying to reflect upon an EDS's positioning on a more abstract level, following the tradition of qualitative research to suggest new concepts that may be used to stipulate further discussion and research. All observations in our data provided us with a rich picture of the storage locations and "information item valuables" that individuals are facing today. These findings indicate that different services are used to purposefully curate specific collections leaving us to wonder how they are interrelated. Based on the deliberate separation of services and the value judgments attached to the information objects, we conclude that different "data value zones" exist that guide the structure of one's PSI (see Figure 1). This concept is grounded in the thematic analysis of our interview data. It serves to illustrate overarching principles describing the perceived zones in an individual's information ecology.

We intend the "data value zones" to serve as a sensitizing concept for further reflections upon the levels where challenges in cloud-storage services might arise if they offer personal storage space that can be shared at the same time. The concept of the "data value zones" also draws upon the metaphor of the information ecology: The zones reflect the habitation (Nardi and O'Day 2000) that means the location of a technology within a network of relationships – from the individual to extended circles. Such circles of sharing and trust have been introduced in social networking services (SNS), for example, in Google+ (Kairam et al. 2012). This enables individuals to control which information items in SNS are shared with which type of audience and what facets (Farnham and Churchill 2011) of an individual are presented on the mediated "stage" of interpersonal communication (Goffman 1959). Our research thus extends this notion of sharing in SNS to any cloud storage services that individuals use to curate information items and possibly want or need to share them. The "data value" zones will be explained in the following.

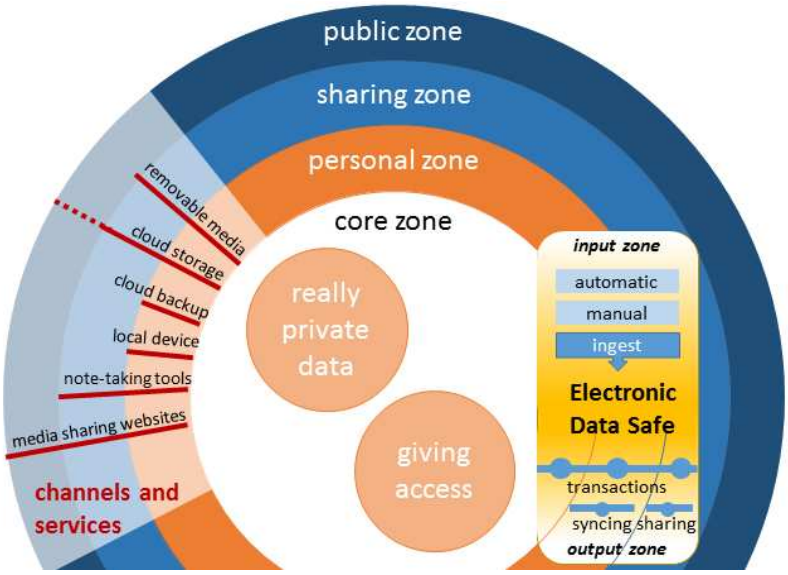

Figure 1: Data value zones

In an individual's core zone, the really private information items are stored, sometimes especially secured by encrypting them, for example with TrueCrypt. In this *core zone*, we place all credentials giving access to other services. Password managers might be used as a supporting tool, thereby implicitly creating an inventory of all digital services in use. The *personal zone* surrounds the core zone as the inmost circle. The content therein is regarded to be personal, either because it is directed from the outside to individuals or it is created by them. Since people are engaged in various social relations, sharing digital information items is performed in the *sharing zone*. Depending upon geographical dispersion, convenience reasons, or other needs, physical or digital storage solutions (cloud storage, SNS, etc.) are used to share items in a controlled zone – or at least giving the impression that the content transferred from the personal zone into the sharing zone is directed and equipped with implicit or explicit rules guiding the privacy of the transferred data to the other party involved. Finally, the *public zone* is dedicated to sharing information items with the general public as an audience for this broadcasting, for example, using media sharing sites or SNS. In the left part the "data value zones" illustration in the grayed area, the services and channels in a personal information ecology are depicted where sharing interactions take place. They may span several zones: for example, cloud storage services offer synchronization of personal data over devices and allow sharing. The previously identified categories of "common" or "selectively stored" documents are not bound to a certain value zone; their placement is bound to the context they are used within or their individually assigned value.

Creating Tensions by Spanning Zones Exemplified by an EDS

An EDS offers services that touch several "data value zones" which will be illustrated in the following. If an EDS's password management functionalities are used, the core zone is involved. An EDS can be used to manage information items in the personal zone and offers functionalities to share data in a (trusted) sharing zone. Furthermore, an EDS has an input zone which also spans the shared zone and the personal zone. Bearing in mind the concept of "data value zones", possibly problematic areas of tension might be identified when services in general touch multiple zones at the same time. For example, the participants in our study reported to be in favor of automatically receiving documents via their EDS; but at the same time, they expressed that these newly arrived documents should fit into their own, personal, organizational scheme which is effective in the personal zone. As we can observe, the transition between the sharing (B2C/G2C) zone into the personal zone could cause tensions. The output zone of an EDS is related to an EDS's capabilities of transferring information items to other zones. For example, synchronization clients might be used in order to securely share data from the personal zone with oneself crossing borders of devices.

If information items need to be shared with others or within electronic transactions, "data value zone" compatible sharing mechanisms are necessary to maintain "contextual integrity", a concept developed by Nissenbaum (2010) and gaining momentum in HCI research (Barkhuus 2012): Privacy is not universally

defined but individually granted depending upon the people involved, the content itself and the context in which the flow of information occurs. With respect to the "data value zones"-concept, this means that any spanning of zones must comply with the individually and context-bound principles to enforce "contextual integrity". To illustrate this, we refer to the subgroup of participants that downloads every information item. Although banking statements might be provided to them via their online banking portal belonging to the shared zone, they mistrust the durability of this sharing and try to bring this information closer to them by storing it in services or on devices that are belonging to the personal zone – which gives them the feeling of having everything under their own control. On the contrary, the laissez-faire types prefer leaving information items on the servers of their providers. Therefore, we conclude that for some collections, parts of the shared zone can be interpreted as an extension of the personal zone. Tensions arise if users experience that their intended placement of information items in zones is not matching the service's handling, for example, by deleting information items without prior notice thereby violating the "contextual integrity". The concept of "data value zones" helps to illustrate on which levels an EDS works and where challenges might arise. In the light of our observations, the tensions of concurrently sharing and safeguarding information items becomes evident in the context of an EDS. Another tension, which has been observed in the field due to transcending "data value zones", is related to an EDS's design for individuals but its shared use.

The tension between sharing and safeguarding, which was independently diagnosed in the recent work by Vertesi et al. (2016) can be confirmed by our observations, especially since our data is based on observations how people store subjectively identified high-value information items. Personal data is often judged to be highly valuable thus needing to be kept in a safe place, for example, an EDS. Nonetheless, people want to share or being able to access these information items in an easy way, for instance, when they are traveling and want to be prepared for a potential loss of identity documents. An EDS should be safe and accessible at the same time. The same applies for documents concerning the last will or the patient will. Replicating the safe space, that means the personal zone, automatically with a synchronization client violates the notion of having something stored safely. In this case, the users' intention of having stored information items safely must be reconsidered since they watch them being distributed over devices. This causes worries: (a) information items might become accessible to someone else when a device is used by someone else, or (b) damaged information items, maybe due to a local virus infection, could be automatically synchronized thereby annihilating the once thought of safe space. These examples illustrate that conflicting needs exist. EDS service providers must creatively resolve this conflicting duality of safeguarding and needs of easy access. Providing mechanisms to control the flow of data to guarantee "contextual integrity" will be a challenge for EDS providers to avoid violating the "data value zones" individuals seem to have. Our work complements Vertesi et al.'s work by suggesting "data value zones" as locations where these tensions may occur and where interventions could be located that need to be designed to minimize or even avoid these tensions.

Further challenges with respect to transcending "data value zones" arise due to the primary design of EDS services being the secure storage location of choice for individuals which is challenged by the observed shared use. Family members were not granted access to an EDS using the "officially" designed functionalities, but they were given access by communicating the master key to the EDS. The same behavior was found in user studies on password sharing which observed that sharing with the family circle is an accepted strategy (Kaye 2011). Especially with regards to next of kin persons, an EDS was conceived as being the digital family archive or the digital equivalent of the paper folders stored in a location that was accessible to any of them. By opening up the whole EDS to others, the core, personal and partly shared "data value zones" are collated into one zone. This should be taken into account by generally all service providers offering person-bound storage services that a single-user design principle does not necessarily reflect actual usage patterns.

With respect to the information ecology concept, our "data value zones" contribute to a refinement and new insights characterizing the constituting elements of an information ecology: (a) system, (b) diversity, (c) coevolution, (d) keystone species, and (e) locality (Nardi and O'Day 2000). We will discuss every element in the following. (a) The *systems* forming part of an information ecology do have strong interrelations. If other services come up with new features (for example, encryption or data centers based in Europe/selectable locations), existing services need to adapt, or they might risk becoming an extinct species. Our findings have shown that users seem to thrive by using multiple services using them for specific tasks and certain facets of managing their information items. (b) The information fragmentation over several services with their specialization can be interpreted as a healthy *diversity* in an information ecosystem. This diversity helps to avoid unhealthy monocultures in the long run, for example by being dependent on only very

few dominating players in the market. (c) Within the group of the "digital filers" that are using advanced scanning equipment, we were able to show that a *coevolution* of services, technologies, and social practices takes place: the whole ecosystem thrives if, for instance, digital filers are using the benefits of modern scanners which might, in turn, lead to further adaptation of technology and/or social practices. This observation highlights the usefulness of describing these activities as practices and understanding these as routines that are shaped and enacted by individuals while technological tools have been used for it or triggered usage. (d) Although being a risk in terms of a monoculture, the big players in the domain of cloud computing for private individuals can also be interpreted as keystone species. Without their efforts of providing ease of use for services and platforms, creating and sustaining demand for further service developments from the users or inhabitants of an ecology system would be slower or not existing. (e) Especially framing and understanding sharing decisions in an information ecology's *locality* as being based on "data value zones" helps service providers to optimize the design of technology in the habitation of PIM practices: As we have demonstrated in our findings, some PIM activities seem to be individual but are, in fact, deeply rooted in social relationships, such as the caring for other family members' information items in one's individual PSI – without having functionalities at hand that take these social ties into account. Furthermore, we demonstrated that the concept of an "information ecology" based on the notion of "practice theory" helps to uncover practices that are shaped by individuals in their use of technology – and that are, in turn, shaping their practices as well.

Limitations

The presented research has been conducted mainly with participants in the Swiss context and a few international participants. Therefore, we assume there might be a cultural bias due to the socially transmitted virtues of being "well organized". Nevertheless, we argue that in explorative research such a bias is negligible. Participants are interacting in their information ecology with internationally rolled-out services and platforms, and we claim therefore that the experiences with an EDS's usage reflect recurrent notions towards safekeeping high-valued information items. For future research, approaching the cultural differences of "getting and being organized" might prove useful, nevertheless. Furthermore, being aware of our qualitative approach, we do not claim universal validity of our findings. Our contributions will help to uncover new problematic areas, which had been left otherwise as blind spots in the service design.

Conclusion

Our study portrayed the use of Electronic Data Safes (EDS). Starting from inside out by analyzing the actual content, the motivations of users and how other cloud-based services are used by them, we gained a deeper understanding how an EDS fits into an individual's information ecology and which practices are developed. This contributes and extends the literature on digital possessions in the context of personal information management (PIM). Our findings show that tensions exist if individuals are aspiring to go for a paperless PIM which entails challenges for practitioners and service providers: (a) assisting users to seamlessly ingest information items to alleviate the problem of information fragmentation, (b) complying with the concurrent user needs to safeguard and share information items, and (c) dealing with a share-everything approach with family members or trusted peers resorting to social trust instead of technology mediation. These challenges need to be addressed by all the actors involved in document or service provision, such as cloud storage providers in general or providers for services that are part of an individual's information ecology. Our developed concept of "data value zones" helps to understand and locate problematic areas of friction that are relevant to all services that offer personal, secure data storage combined with data sharing capabilities. Such services touch the users' perception of data value and privacy, and they must bring additional value in an individual's information ecology by reducing frictions and information fragmentation.

Acknowledgements

The authors would like to thank the interview participants for their time and sharing their experiences. Also, we would like to thank the two Swiss-based service providers for electronic data safes in helping us to recruit interview participants and offering the small gift to the participants. Furthermore, we thank the anonymous reviewers for their constructive feedback.

References

Barkhuus, L. 2012. "The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 367–376 (doi: 10.1145/2207676.2207727).

Blevis, E., Bødker, S., Flach, J., Forlizzi, J., Jung, H., Kaptelinin, V., Nardi, B., and Rizzo, A. 2015. "Ecological Perspectives in HCI: Promise, Problems, and Potential," in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '15, New York, NY, USA: ACM, pp. 2401–2404 (doi: 10.1145/2702613.2702634).

Boardman, R., and Sasse, M. A. 2004. "'Stuff goes into the computer and doesn't come out': a cross-tool study of personal information management," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, New York, NY, USA: ACM, pp. 583–590 (doi: 10.1145/985692.985766).

Bødker, S., and Klokmose, C. N. 2012. "Dynamics in Artifact Ecologies," in *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*. NordiCHI '12, New York, NY, USA: ACM, pp. 448–457 (doi: 10.1145/2399016.2399085).

Borgmann, M., Hahn, T., Herfert, M., Kunz, T., Richter, M., Viebeg, U., and Vowé, S. 2012. "On the Security of Cloud Storage Services," No. SIT-TR-2012-001, Darmstadt: Fraunhofer Institute for Secure Information Technology SIT (available at http://www.sit.fraunhofer.de/content/dam/sit/en/studies/Cloud-Storage-Security_a4.pdf).

Braun, V., and Clarke, V. 2006. "Using thematic analysis in psychology," *Qualitative Research in Psychology* (3:2), pp. 77–101 (doi: 10.1191/1478088706qp063oa).

Breitenstrom, C., Brunzel, M., and Klessmann, J. 2008. "Elektronische Safes für Daten und Dokumente," White Paper, , Berlin: Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS) (available at http://www.fokus.fraunhofer.de/de/elan/_docs/_hpp-gruppe/esafe_white-paper_081219.pdf).

Capra, R., Vardell, E., and Brennan, K. 2014. "File synchronization and sharing: User practices and challenges," *Proceedings of the American Society for Information Science and Technology* (51:1), pp. 1–10 (doi: 10.1002/meet.2014.14505101059).

Cecez-Kecmanovic, D., Galliers, R. D., Henfridsson, O., Newell, S., and Vidgen, R. 2014. "The sociomateriality of information systems: current status, future directions," *MIS Quarterly* (38:3), pp. 809–830.

Cushing, A. L. 2012. "Possessions and self extension in digital environments: implications for maintaining personal information," University of North Carolina at Chapel Hill.

Davenport, T. H., and Prusak, L. 1997. *Information Ecology: Mastering the Information and Knowledge Environment* (1st ed.), Oxford University Press.

Dearman, D., and Pierce, J. S. 2008. "It's on my other computer!: computing with multiple devices," in *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, New York, NY, USA: ACM, pp. 767–776 (doi: 10.1145/1357054.1357177).

Farnham, S. D., and Churchill, E. F. 2011. "Faceted identity, faceted lives: social and technical issues with being yourself online," in *Proceedings of the ACM 2011 conference on Computer supported cooperative work*. CSCW '11, New York, NY, USA: ACM, pp. 359–368 (doi: 10.1145/1958824.1958880).

Fidel, R. 2012. *Human Information Interaction: An Ecological Approach to Information Behavior*, MIT Press.

Glaser, B. G., and Strauss, A. L. 2009. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Transaction Publishers.

Goffman, E. 1959. *The presentation of self in everyday life*. A Doubleday Anchor book, Garden City, N.Y: Doubleday.

Hawkins, D. T., and Kahle, B. 2013. *Personal Archiving: Preserving Our Digital Heritage*, Medford, New Jersey: Information Today Inc.

Hicks, B. J., Dong, A., Palmer, R., and Mcalpine, H. C. 2008. "Organizing and managing personal electronic files: A mechanical engineer's perspective," *ACM Trans. Inf. Syst.* (26:4), p. 23:1–23:40 (doi: 10.1145/1402256.1402262).

Hildebrand, D. 2015. "E-invoicing as the Principal Driver of Change in B2X Letter Market Definitions," in *Postal and Delivery Innovation in the Digital Economy*. M. A. Crew and T. J. Brennan (eds.), Cham: Springer International Publishing, pp. 277–289 (available at http://link.springer.com/10.1007/978-3-319-12874-0_21).

Hoffmann, M., and Jäppinen, P. 2013. "Introducing Life Management Platforms and Collaborative Service Fusion to Contextual Environments," in *Cyber Security and Privacy*. M. Felici (ed.), Springer Berlin, pp. 41–52 (available at http://link.springer.com/chapter/10.1007/978-3-642-41205-9_4).

International Post Corporation. 2015. "Global Postal Industry Report 2015 - Key Findings," International Post Corporation (available at https://www.ipc.be/~/media/documents/public/markets/mi%20products/ipc_gpir2015_key_findings.pdf).

Jones, W. 2012. *The Future of Personal Information Management, Part 1: Our Information, Always and Forever*, Morgan & Claypool (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6813158).

Jones, W. 2013. *Transforming Technologies to Manage Our Information:The Future of Personal Information Management, Part 2*, Morgan & Claypool (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6812958).

Jones, W. 2015. *Building a Better World with Our Information: The Future of Personal Information Management, Part 3*, Morgan & Claypool (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7240060).

Jones, W., and Bruce, H. 2005. "A Report on the NSF-Sponsored Workshop on Personal Information Management, Seattle, WA, 2005," (available at http://pim.ischool.washington.edu/final%20PIM%20report.pdf).

Jones, W. P. 2008. *Keeping found things found: the study and practice of personal information management*, Morgan Kaufmann.

Jones, W., and Teevan, J. 2007. *Personal Information Management*, University of Washington Press.

Jung, H., Stolterman, E., Ryan, W., Thompson, T., and Siegel, M. 2008. "Toward a Framework for Ecologies of Artifacts: How Are Digital Artifacts Interconnected Within a Personal Life?," in *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges*. NordiCHI '08, New York, NY, USA: ACM, pp. 201–210 (doi: 10.1145/1463160.1463182).

Kairam, S., Brzozowski, M., Huffaker, D., and Chi, E. 2012. "Talking in Circles: Selective Sharing in Google+," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '12, New York, NY, USA: ACM, pp. 1065–1074 (doi: 10.1145/2207676.2208552).

Karger, D. R. 2007. "Unify Everything: It's all the Same to Me," in *Personal Information Management*. W. P. Jones and J. Teevan (eds.), University of Washington Press, pp. 127–152.

Kaye, J. J., McCuistion, M., Gulotta, R., and Shamma, D. A. 2014. "Money talks: tracking personal finances," ACM Press, pp. 521–530 (doi: 10.1145/2556288.2556975).

Kaye, J. "Jofish." 2011. "Self-reported Password Sharing Strategies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 2619–2622 (doi: 10.1145/1978942.1979324).

Kaye, J. "Jofish," Vertesi, J., Avery, S., Dafoe, A., David, S., Onaga, L., Rosero, I., and Pinch, T. 2006. "To have and to hold: exploring the personal archive," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, New York, NY, USA: ACM, pp. 275–284 (doi: 10.1145/1124772.1124814).

Klein, H. K., and Myers, M. D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), p. 67 (doi: 10.2307/249410).

Klieme, E., Strick, L., Wunderlich, W., Braun, J., and Wiesmaier, A. 2011. "Der elektronische Safe als vertrauenswürdiger Cloud Service," ISPRAT.

Kuppinger, M., and Kearns, D. 2013. "Life Management Platforms: Control and Privacy for Personal Data," in *Digital enlightenment yearbook 2013: the value of personal data*. M. Hildebrandt, K. O'Hara, and M. Waidner (eds.), Amsterdam: IOS Press, pp. 243–252 (available at http://ebooks.iospress.nl/isbn/978-1-61499-295-0).

Kuutti, K. 2013. "'Practice turn' and CSCW identity," *ECSCW 2013 Adjunct Proceedings* (available at http://ojs.statsbiblioteket.dk/index.php/daimipb/article/download/13587/11586#page=47).

Kvavilashvili, L., and Ellis, J. 2004. "Ecological validity and the real-life/laboratory controversy in memory research: A critical (and historical) review," *History and Philosophy of Psychology* (6), pp. 59–80.

Lee, C. A. 2011. *I, Digital: Personal Collections in the Digital Era*, American Library Association.

Malone, T. W. 1983. "How do people organize their desks?: Implications for the design of office information systems," *ACM Trans. Inf. Syst.* (1:1), pp. 99–112 (doi: 10.1145/357423.357430).

Marshall, C. 2007. "How people manage personal information over a lifetime," in *Personal Information Management*. W. Jones and J. Teevan (eds.), University of Washington Press, pp. 153–166.

Marshall, C. 2008a. "Rethinking Personal Digital Archiving, Part 1," *D-Lib Magazine* (14:3/4) (doi: 10.1045/march2008-marshall-pt1).

Marshall, C. 2008b. "Rethinking Personal Digital Archiving, Part 2," *D-Lib Magazine* (14:3/4) (doi: 10.1045/march2008-marshall-pt2).

Marshall, C. 2011. "Challenges and Opportunities for Personal Digital Archiving," in *Personal Collections in the Digital Era*, Chicago, IL: Society of American Archivists, pp. 90–114 (available at http://www.csdl.tamu.edu/~marshall/I-Digital-Marshall.pdf).

Marshall, C., and Tang, J. C. 2012. "That syncing feeling: early user experiences with the cloud," in *Proceedings of the Designing Interactive Systems Conference*, New York, NY, USA: ACM, pp. 544–553 (doi: 10.1145/2317956.2318038).

Mayer-Schönberger, V. 2007. "Useful void: The art of forgetting in the age of ubiquitous computing," *KSG Working Paper No. RWP07-022*.

McKemmish, S. 2001. "Placing records continuum theory and practice," *Archival science* (1:4), pp. 333–359.

McKemmish, S., and Piggott, M. 1994. *The records continuum: Ian Maclean and Australian Archives : first fifty years*, Clayton: Ancora Press.

Nardi, B. A., and O'Day, V. L. 2000. *Information ecologies: using technology with heart* (1. MIT Press paperback ed.), Cambridge, Mass.: MIT Press.

Nissenbaum, H. F. 2010. *Privacy in context: technology, policy, and the integrity of social life*, Stanford, Calif.: Stanford Law Books.

Odom, W., Sellen, A., Harper, R., and Thereska, E. 2012. "Lost in translation: understanding the possession of digital things in the cloud," in *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 781–790 (doi: 10.1145/2207676.2207789).

Pfister, J., and Schwabe, G. 2013. "The Landscape of Electronic Data Safes and Their Adoption in E-Government and E-Business," in *2013 46th Hawaii International Conference on System Sciences (HICSS)*, pp. 1963–1972 (doi: 10.1109/HICSS.2013.532).

Pfister, J., and Schwabe, G. 2015. "Electronic Data Safes as an Infrastructure for Transformational Government? A Case Study," in *Electronic Government, 14th IFIP WG 8.5 International Conference, EGOV 2015, Thessaloniki, Greece, August 30 -- September 2, 2015, Proceedings*. E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, B. Klievink, I. Lindgren, and P. Parycek (eds.), Springer International Publishing, pp. 246–257 (available at http://link.springer.com/chapter/10.1007/978-3-319-22479-4_19).

Schatzki, T. R., Knorr-Cetina, K., and Savigny, E. von. 2001. *The practice turn in contemporary theory*, London; New York: Routledge (available at http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=134021).

Schulz, S., Hoffmann, C., Klessmann, J., Penski, A., and Warnecke, T. 2010. "Dienste auf Basis elektronischer Safes für Daten und Dokumente," Lorenz-von-Stein-Institut, Fraunhofer FOKUS.

Sellen, A. J., and Harper, R. H. R. 2002. *The myth of the paperless office*, Cambridge, Mass: MIT Press.

Strauss, A., and Corbin, J. M. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, SAGE.

Tang, J. C., Brubaker, J. R., and Marshall, C. C. 2013. "What Do You See in the Cloud? Understanding the Cloud-Based User Experience through Practices," in *Human-Computer Interaction – INTERACT 2013*Lecture Notes in Computer Science, P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson, and M. Winckler (eds.), Springer Berlin Heidelberg, pp. 678–695 (available at http://link.springer.com/chapter/10.1007/978-3-642-40480-1_47).

Tavakoli, A., and Schlagwein, D. 2016. "A REVIEW OF THE USE OF PRACTICE THEORY IN INFORMATION SYSTEMS RESEARCH," in *Proceedings of the Pacific Asia Conference on Information Systems*. P. Y. K. Chau and C. She-I (eds.), Presented at the PACIS, Chiayi, Taiwan (available at www.pacis2016.org/Abstract/ALL/553.pdf).

Thomson, L. 2013. "'When i've packed it in and they send me something …': Information boundaries in professional home offices," *Proceedings of the American Society for Information Science and Technology* (50:1), pp. 1–5 (doi: 10.1002/meet.14505001158).

Vertesi, J., Kaye, J., Jarosewski, S. N., Khovanskaya, V. D., and Song, J. 2016. "Data Narratives: Uncovering Tensions in Personal Data Management," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, New York, NY, USA: ACM, pp. 478–490 (doi: 10.1145/2818048.2820017).

Vincent, C. J., Li, Y., and Blandford, A. 2014. "Integration of human factors and ergonomics during medical device design and development: It's all about communication," *Applied Ergonomics* (45:3), pp. 413–419 (doi: 10.1016/j.apergo.2013.05.009).

Voida, A., Olson, J. S., and Olson, G. M. 2013. "Turbulence in the Clouds: Challenges of Cloud-based Information Work," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '13, New York, NY, USA: ACM, pp. 2273–2282 (doi: 10.1145/2470654.2481313).

Watkins, R. D., Sellen, A., and Lindley, S. E. 2015. "Digital Collections and Digital Collecting Practices," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15, New York, NY, USA: ACM, pp. 3423–3432 (doi: 10.1145/2702123.2702380).

Wegner, D. M. 1987. "Transactive Memory: A Contemporary Analysis of the Group Mind," in *Theories of Group Behavior*. B. Mullen and G. R. Goethals (eds.), Springer New York, pp. 185–208 (available at http://link.springer.com/chapter/10.1007/978-1-4612-4634-3_9).

Whittaker, S. 2011. "Personal information management: From information consumption to curation," *Annual Review of Information Science and Technology* (45:1), pp. 1–62 (doi: 10.1002/aris.2011.1440450108).

Wilson, T. D. 2000. "Human information behavior," *Informing science* (3:2), pp. 49–56.

Xie, X., Sonnenwald, D. H., and Fulton, C. 2015. "The role of memory in document re-finding," *Library Hi Tech* (33:1), pp. 83–102 (doi: 10.1108/LHT-06-2014-0050).

Yvette Blount. 2011. "Employee management and service provision: a conceptual framework," *Information Technology & People* (24:2), pp. 134–157 (doi: 10.1108/09593841111137331).